UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/801,363	03/15/2004	Jochen Weber	10191/3602	3174

26646 7590 04/03/2007
KENYON & KENYON LLP
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER	
TRAORE, FATOUMATA	

ART UNIT	PAPER NUMBER
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/03/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

8

Office Action Summary	**Application No.** 10/801,363	**Applicant(s)** WEBER ET AL.
	Examiner Fatoumata Traore	**Art Unit** 2109

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *15 March 2004*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *15 March 2004* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is in response of the original filing of March 15, 2004. Claims 1-19 are pending and have been considered below.

Claim Objections

2. Claims 4, 11 are objected to because of the following informalities: claim 4 reads the limitation of "save" and claim 11 reads the limitation of "unsymmetrical " which are believe to be grammatical errors, the examiner interpreted them respectively as "same", "asymmetric". Appropriate correction is required.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1, 9, 10, 17 are rejected under 35 U.S.C. 102(b) as being anticipated by **Gilley et al** (US 5771287).

Claim 1: **Gilley et al** discloses an apparatus for controlling the feature set of a programmable device comprising:

A plurality of modules including a microprocessor and at least one storage module for storing code and data for the microprocessor, at least one of the modules storing a serial number of the at least one module in a non-exchangeable manner (a database which is correlates and stores a set of programmable device serial number) (column 4, lines 34-36);

An arrangement for storing a code number, the code number being obtained from the serial number by using an encryption method, and for storing information required to calculate the serial number form the code number (each programmable device, uniquely identified by a serial number, has a secure memory location to store the secret key associated with it serial number. Both the programming device and each programmable device include memory with a program that uses a secure cryptographic method to calculate authentication codes) (column 4, lines 36-49),

Wherein the microprocessor is adapted to calculate a serial number from the code number on the basis of the information to compare the calculated serial number to the stored serial number, and to execute or not execute at least part of the code as a function of a result of the comparison (This present authentication code is then compared by the programmable device to the factory calculated and set authentication code that was originally stored in the programmable device memory. If the two authentication codes match, the programmable device will authorize to function with the present feature set by the present operation mode code. If they do not match, the programmable takes a number of different actions, including refusing to conduct certain functions, refusing to operate at all, or defaulting to a lower feature set) (column 4, lines 22-34).

Claim 9: **Gilley et al** discloses an apparatus for controlling the feature set of a programmable device and preventing tampering with memory in electronic device as in claim 1 above, and **Gilley et al** further discloses that at least two of the modules are each identified by a serial number and the code number is obtained by joint encryption of the serial numbers (Both the EEPROM and ROM contain serial number SN) (column 6, lines 30-60, figure 1).

Claim 10: **Gilley et al** discloses a method for controlling the feature set of a programmable device comprising:

Storing, in the microprocessor system, a code number, which is obtained from the serial number by using an encryption method, and storing information required for calculating the serial number from the code number (each programmable device, uniquely identified by a serial number, has a secure memory location to store the secret key associated with it serial number. Both the programming device and each programmable device include memory with a program that uses a secure cryptographic method to calculate authentication codes) (column 4, lines 36-49);

Reading the code number and calculating an unencrypted serial number from the code number with the aid of the information (the authentication code is calculated using the operation mode code and the secret key together with a cryptographic methodology. This authentication code is then also programmed in a programmable device's memory. It does not have to be secured) (column 4, lines 12-6);

Comparing the decrypted serial number thus obtained with the serial number of the module (This present authentication code is then compared by the programmable device to the factory calculated and set authentication code that was originally stored in the programmable device memory) (column 4, lines 22-30);

And detecting an exchange of the module if the serial number of the module does not match the decrypted serial number (If the two authentication codes match, the programmable device will authorize to function with the present feature set by the present operation mode code. If they do not match, the programmable takes a number of different actions, including refusing to conduct certain functions, refusing to operate at all, or defaulting to a lower feature set) (column 4, lines 26-34).

Claim 17: **Gilley et al** discloses a method for controlling the feature set of a programmable device and preventing tampering with memory in electronic device as in claim 10 above, and **Gilley et al** further discloses that the method is used for a plurality of modules of the microprocessor system and the code number is obtained by a joint encryption of serial numbers of the plurality of modules the module includes a microprocessor of the microprocessor system (a secure encryption algorithm is used with the operation mode code and the secret key to create the authentication code) (column 5, lines 66-67 and column 6 lines 1-5).

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claims 2-8, 11-16, 18, 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gilley et al (US5771287) in view of Osborn (US 6026293).

Claims 2, 11: **Gilley et al** discloses a apparatus and method for controlling the feature set of a programmable device as in claims 1 and 10 above, but does not disclose that a asymmetric encryption method is used. However, **Osborn** discloses an apparatus for preventing tampering with memory in electronic device, which further discloses an asymmetric authentication (data transfer device authentication involves the use of a public/private key authentication scheme) (column 6, lines 50-53). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to add asymmetric encryption in **Gilley et al**. One would have been motivate to do so in order to maintain system security.

Claims 3, 12: **Gilley et al** and **Osborn** disclose an apparatus and method for controlling the feature set of a programmable device and preventing tampering with memory in electronic device as in claims 2 and 10 above, and **Gilley et al** further discloses that one of the at least one module identified by the serial number is a storage module (figure 1).

Claims 4, 13: **Gilley et al** and **Osborn** disclose an apparatus and method for controlling the feature set of a programmable device and preventing tampering with memory in electronic device as in claims 3 and 12 above, and **Gilley et al** further discloses that the code number is stored in a same storage module as the serial number (the read only memory contains the serial, the code to enable the scrambling function) (column 6, lines 53-57 and Figure 1).

Claims 5, 14: **Gilley et al** and **Osborn** disclose an apparatus and method for controlling the feature set of a programmable device and preventing tampering with memory in electronic device as in claims 3 and 12 above, and **Gilley et al** further discloses that the storage module is an electrically rewritable, non-volatile memory (scrambler also utilizes an electrically erasable programmable read only memory) (column 5, lines 31-3), and the code to be executed if the calculated and the stored serial numbers do not match includes a command for deletion of the storage module (If the two authentication codes match, the programmable device will authorize to function with the present feature set by the present operation mode code. If they do not match, the programmable takes a number of different actions, including refusing to conduct certain functions, refusing to operate at all, or defaulting to a lower feature set, other action are possible (deletion of storage module)) (column 4, lines 26-34).

Claims 6, 15: **Gilley et al** discloses an apparatus and method for controlling the feature set of a programmable device and preventing tampering with memory in electronic device as in claims 1 and 10 above, but does not explicitly disclose that one of the at least one module identified by the serial number is the microprocessor. However, **Osborn** discloses an apparatus for preventing tampering with memory in electronic device, which further discloses a microprocessor as one of the module identified by the serial number (figure 4). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to add the step of identifying the microprocessor by the serial number in **Gilley et al**. One would have been motivate to do so in order to maintain system security.

Claims 7, 16: **Gilley et al** discloses an apparatus and method for controlling the feature set of a programmable device and preventing tampering with memory in electronic device as in claims 1 and 10 above, but does not explicitly disclose that the information required to calculate the serial number from the code number is stored in a different storage module than the code number. However, **Osborn** discloses an apparatus for preventing tampering with memory in electronic device, which further discloses that the information required to calculate the serial number from the code number is stored in a different storage module than the code number (the Internal Read Only Memory IROM contains boot code, hashing code, authentication code and public encryption key, The Electronically Erasable Programmable Read Only Memory (EEPROM) includes user profile data, and Electronic Serial Number (ESN) (column 7 line 67 and column 8, lines 1-7). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to add the step of storing the information required to calculate the serial in a different module in **<u>Gilley et al</u>**. One would have been motivate to do so in order to maintain system security.

Claim 8: **<u>Gilley et al</u>** and **Osborn** disclose an apparatus for controlling the feature set of a programmable device and preventing tampering with memory in electronic device as in claim 7 above, and **<u>Gilley et al</u>** further discloses the different storage module is connected to the microprocessor in a non-separable manner (scramble includes a microprocessor, an electrically erasable programmable read only memory and a read only memory) (column 5, lins29-35).

Claim 18: **<u>Gilley et al</u>** discloses an method for controlling the feature set of a programmable device and preventing tampering with memory in electronic device as in claim 10 above, but does not explicitly disclose that steps of the method are executed upon each start-up of the microprocessor system. However, **<u>Osborn</u>** discloses an apparatus for preventing tampering with memory in electronic for preventing tamp device, which further discloses that steps of the method are executed upon each start-up of the microprocessor system (A process for telephone power up and memory validation for the system depicted in Fig 4, according to an exemplary embodiment of the invention, is illustrated in Fig 5. After the cellular telephone is turned on, boot code within the Internal Read Only Memory (IROM) is executed by the microprocessor to initialize the controller. Has code containing in the IROM is then run to perform an audit hash value calculation over selected contents of the flash program and the Electronic Serial Number (ESN) value stored in EEPROM) (column 8, lines 19-30). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to add the steps of execution of the method at each start-up in **Gilley et al**. One would have been motivate to do so in order to maintain system security.

Claim 19: **Gilley et al** discloses an method for controlling the feature set of a programmable device and preventing tampering with memory in electronic device as in claim 10 above but does not explicitly disclose that steps of the method are periodically executed during operation of the microprocessor system. However, **Osborn** discloses an apparatus for preventing tampering with memory in electronic device, which further discloses that steps of the method are periodically executed during operation of the microprocessor system (a periodic hash value calculation process is enabled, whereafter the cellular telephone begins normal operation) (column 8, lines 38-40). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to add the steps of a periodical execution of the method in **Gilley et al**. One would have been motivate to do so in order to maintain system security.

Conclusion

1. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. Lee et al (US 5774544) Method and apparatus for encrypting and decrypting microprocessor serial numbers.

b. Smith (US 4731842) Security module for electronic funds transfer system.

c. Leonardi (US 6556680) Method for authorization check.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685. The examiner can normally be reached Monday through Thursday from 7:30 a.m. to 4:30 p.m. and every other Friday from 7:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jim W. Myhre, can be reached on (571) 272 6722. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-3800. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 274-1685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

FT
March 21, 2007

James W. Myhre
Supervisory Patent Examiner